Environmental Management Consolidated Business Center (EMCBC)

Subject: Configuration Management of Computer Systems and Networks

Implementing Procedure APPROVED: ***(Signature on File)***
EMCBC Director
ISSUED BY: OFFICE OF INFORMATION RESOURCE MANAGEMENT

1.0 PURPOSE

The purpose of this procedure is to define the methods and process to control the configuration of all components that define the cyber security boundary of EMCBC Information Technology (IT) systems.

2.0 SCOPE

All IT functions within the EMCBC and all Sites utilizing EMCBC network systems or managed hardware.

3.0 APPLICABILITY

This procedure is applicable to all IT processes and systems managed by the EMCBC Office of Information Management. This procedure is not applicable to systems connecting to the EMCBC "hotel type" internet provided for visitors.

4.0 REFERENCES

4.1 PL-240-08 Cyber Security – System Security Plan for General Support System
- 4.1.1 AC-5 Separation of Duties
- 4.1.2 AC-6 Least Privilege
- 4.1.3 CM-1 Configuration Management Policy and Procedures
- 4.1.4 CM-2 Baseline Configuration
- 4.1.5 CM-3 Configuration Change Control
- 4.1.6 CM-4 Monitoring Configuration Changes
- 4.1.7 CM-5 Access Restrictions for Change
- 4.1.8 CM-6 Configuration Setting
- 4.1.9 CM-7 Least Functionality
- 4.1.10 MA-3 Maintenance Tools
- 4.1.11 RA-1 Risk Assessment Policy and Procedures
- 4.1.12 RA-4 Risk Assessment Update
- 4.1.13 SA-1 System and Services Acquisition Policy and Procedures
- 4.1.14 SA-3 Life-Cycle Support
- 4.1.15 SA-10 Developer Configuration Management
- 4.1.16 SA-11 Developer Security Testing
- 4.1.17 SC-1 System and Communications Protection Policy and Procedures

4.1.18 SC-14 Public Access Protections

5.0 DEFINITIONS

5.1 Cognizant Assistant Director: Assistant Director that is the controlling subject matter expert for a given application.

5.2 ADIRM: Assistant Director for Information Management, EMCBC.

5.3 System Owner: The non IRM individual that is responsible for the function that a particular application is performing.

5.4 Configuration Control Point Manager: The IRM staff member responsible for a particular Configuration Control Point.

5.5 Technical Owner: IRM staff member responsible for a particular application.

5.6 Member at Large: Member of the IRM staff who is not the Configuration Control Point Manager who is appointed by the ADIRM for the purposes of serving on the Configuration Control Board.

5.7 Technical Documents: Internal Technical Documents controlled by Information Resource Management in accordance with written procedure.

6.0 RESPONSIBILITIES

6.1 Assistant Manager for Information Resource Management
- 6.1.1 Chairs the Configuration Control Board
- 6.1.2 Approves Configuration Baseline Changes
- 6.1.3 Approves Configuration Checklists

6.2 Configuration Control Point Manager
- 6.2.1 Manage the Configuration of their assigned control point
- 6.2.2 Develop Baseline Changes as appropriate
- 6.2.3 Ensure that noted risks are updated in the Electronic Risk Assessment Management System (eRAMS)

7.0 GENERAL INFORMATION

The configuration management plan is structured to address the different aspects of the many computer systems that make up the EMCBC IT infrastructure. Information Management has many diverse elements, from Blackberry handhelds to servers handling multiple databases. This procedure provides for processes to establish baselines for each of the main configuration areas and then provides for controlled change and expansion of the system to meet the growing IT service area of the EMCBC. The plan provides for methods where security configurations are not defined by specific benchmarks, but where there is technical literature that will support development of secure configurations.

8.0 PROCEDURE

8.1 Baselines – Initial Baselines are established at the time of Certification and Accreditation or may be subsequently established as new hardware, software or new applications are added to the system.

8.1.1 Development of Initial Baselines - Baselines are developed by the application of DOE standard configurations, as in the case of the DOE Common Operating Environment for desktops, or the use of benchmarks such as CIS (Center for Internet Security), and DISA (Defense Information Security Agency) standards for Servers, or if standards or benchmarks do not exist IRM will develop a baseline configuration based on industry understanding of risks as outlined in trade literature (for example: the disabling the use of "magic quotes" in PHP, (a hypertext language). Such in-house baseline checklists will be documented in the form of a **Technical Document** and will be reviewed periodically to ensure that new risks are addressed and added to the checklist.

8.2 Configuration Management - The EMCBC Configuration Management system is separated into four distinct Configuration Control Points (CCP), Desktops, Servers, Network configuration, and Applications. Each Configuration Control Point will be assigned a Manager. The CCP Manager is responsible for ensuring that their CCP meets the requirement of this procedure.

8.2.1 Desktop Configuration – The EMCBC uses the DOE Common Operation Environment (DOECOE) as the baseline configuration for all desktops. The DOECOE is updated as versions are issued by the Office of the Chief Information Officer (OCIO). In addition, EMCBC may deploy additional software over and above the standard software suite provided by the DOECOE. These additions will be documented and approved by the Assistant Director for Information Resource Management (ADIRM) and documented as risks if appropriate in eRAMS.

8.2.1.1 Laptops – Laptop configurations are developed by manufacturing type. The CIS standards establish laptop configuration. Users are allowed limited administrative rights on laptops to facilitate their use off site.

8.2.2 Server Configuration – The EMCBC uses CIS and DISA benchmarking tools to establish baselines for Server Configurations.

8.2.2.1 Each server will be benchmarked to the appropriate tools based on the function of the server. For example the web-server may have a different benchmark score than the server used to support the CBC-intranet.

8.2.2.2 Minimum scoring levels will be established by the ADIRM in accordance with guidance from DOE Headquarters or based on industry standards.

8.2.2.3 Additional Server Configurations are established based on Database Management Systems or web services that "sit" on top of the Windows Server software. These included such software as PHP, Microsoft SQL Database Manager (MSSQL), open source database manager (MySQL), etc. This type of software is baselined by using the checklist method if benchmarks are not available. Configurations files, such as .ini files are maintained as the configuration settings for the software.

8.2.3 Network Configuration – Network configuration is documented by a network diagram showing the interconnections of the network and by documentation of the settings of the security equipment, such as firewalls, router, intrusion detections equipment, etc.

8.2.3.1 The Network Diagram is approved by the ADIRM and the settings on all network appliances are established and approved using the Baseline Configuration Change Form. Note that for clarifications the Voice Over Internet Protocol (VoIP) phones are considered to be a network item (because besides being a phone they are a switch) while the VoIP Server (MGCs) are controlled through server configuration control.

8.2.4 Application Configuration (EMCBC) – Applications Baselines are established by application of security checklist. These types of checklist establish requirements for coding standards and address issues such as code injection attacks and information control.

8.2.4.1 IRM will maintain a list of the version of the software, the status, and the results of latest configuration checklist. This requirement only applies to EMCBC developed or maintained applications.

8.3 Baseline Configuration Change – Baseline changes are developed and documented on a Baseline Change Form. Anyone working on a project or application may develop a change.

8.3.1 The proposed change is reviewed by the Configuration Control Board (CCB) made up of the ADIRM (Chair), the Configuration Control Point Manager, and one other member of the IRM support staff. Changes may be accepted, rejected, or put on holding pending the need for additional information or the need for off network testing.

8.3.2 The CCB will determine if the system or application needs to be re-baselined by application of the checklist or rerunning of a benchmark tool.

8.3.3 The CCB will also determine if there is any residual risk that requires documentation in eRAMS. The Manager of the Configuration Control Point will be responsible for ensuring that the risks in eRAMS are updated.

8.3.4 The CCB will determine if the change will impact the Interconnect agreement with DOENet (and thus require completion of HQ CCP form).

8.3.5 The CCB will determine if the change will significantly impact any work process guided by a procedure or plan or other EMCBC document.

8.3.6 All members of the review board will sign the Baseline Change Form.

8.3.7 All changes made as a result of the CCB will be forwarded to the CCP Manager. The CCP Manager will ensure that once activated or installed all approved Baseline Configuration Change are documented in the Maintenance Log.

8.3.8 Each CCP Manager shall ensure that the Least Functionality in accordance with PL-240-08, Cyber Security – System Security Plan for General Support System, is being maintained.

8.4 Minor Changes – Often during the course of system operations minor changes need to be made to options or settings of various hardware, software or applications to improve the functionality of the system or applications. These changes may be made by cognizant IRM staff to existing applications in the Configuration Baseline.

8.4.1 These types of changes are to be documented in the Maintenance Log. The Log will be reviewed weekly to ensure that major changes that may affect the security posture have not been made without proper review.

8.4.2 A quarterly review will be conducted to determine if the aggregate effect of the minor changes requires base lining activity.

8.5 Maintenance Log - All actions such as changes, reviews, and audits, associated with the EMCBC Information Systems are documented in the Maintenance Log. Items that change configurations are indicated as such in the Log.

9.0 RECORDS MAINTENANCE

9.1 Records generated as a result of implementing this document are identified as follows:

9.1.1 Configuration Change Proposal - Baseline Change Form, IP-240-02-F1, Rev. 1

9.1.2 IM Maintenance Log

10.0 FORMS USED – All Forms are the latest revision unless otherwise specified.

10.1 Configuration Change Proposal – Baseline Change Form, IP-240-02-F1, Rev. 1

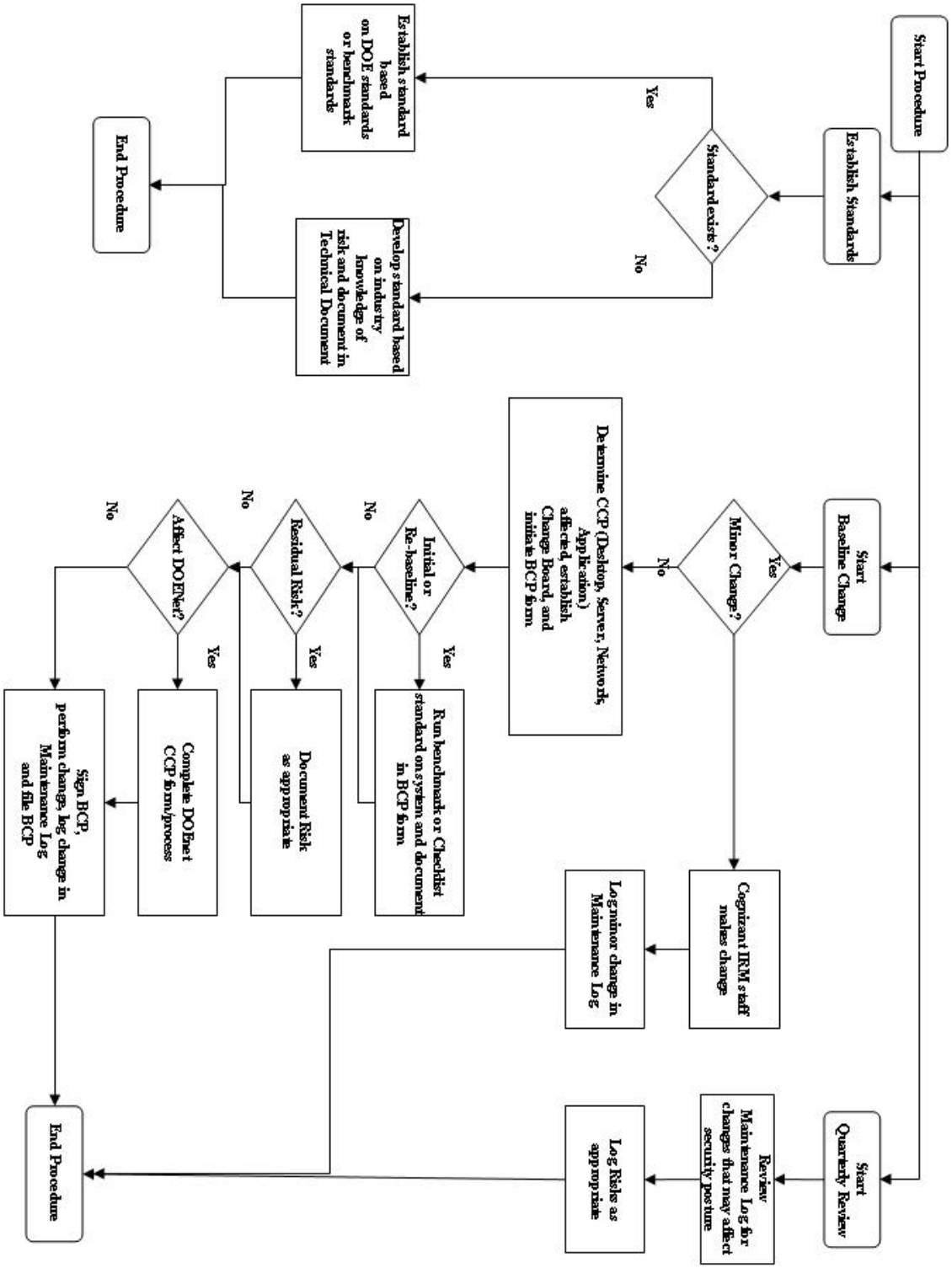
10.2 IM Maintenance Log

11.0 ATTACHMENTS

11.1 Attachment A - Configuration Change Proposal – Baseline Change Form, IP-240-02-F1, Rev. 1

11.2 Attachment B - IM Maintenance Log

12.0 FLOWCHART



Attachment A

CM Information Resource Management EMCBC	**Configuration Change Proposal –Baseline Change**	Control Point:
	No. BCP-2007-001	Date

Proposed Change

Additional Testing or Baseline Testing required? Yes __ No __
Does this Change affect Interconnect with DOENet? Yes __ No __
Does this Change significantly affect any documents, procedures, or plans?
Yes __ No __

Impacted Systems and Applications:

APPROVED ___ REJECTED___ HOLD ___	ERAMS UPDATE REQUIRED ☐
Assistant Director for IRM	Date
Control Point Manager	Date
Member at Large:	Date

Attachment B

EMCBC MAINTENANCE LOG

Add New

Control Point	System Name	Action	Date	Co Ch
Logs	PIT	Unusual Traffic Alert - Dan Bright reported seeing	2006-11-03	No
Logs	COOP	HVAC Break down - Based on the break down of HVAC	2006-10-27	No
Logs	CBCFS1	Gave Betsy Volk special permissions to the sb07 fo	2006-10-27	No
Network	CBCSQL	Changed the IP address that is allowed to authenti	2006-10-18	Yes
Audit	Active	Reviewed active dir accounts 10/2006 disabled G G	2006-10-17	No
Audit	Desktop	Verified that the vml exploitation would not affec	2006-10-05	No
Network	CBCCORE1 & CBCCORE2	Change route to include a route to HQ DNS.	2006-07-17	Yes
Server	CBCINTRANET	Changed in PHP.ini SMTP=localhost to SMTP=cbcexch1	2006-06-29	Yes
Server	CBCMGC1	Upgrade Sphericall to 4.0.2.13 and install patch s	2006-06-19	Yes
Server	CBCSQL	AdminToolPack from Microsoft downloaded and instal	2006-06-16	Yes
Logs	CBCSQL	1st SMS Package Released and Successfully Pushed t	2006-06-14	No
Server	CBCSQL	SMS Toolkit for SP2	2006-06-14	No
Server	CBCSQL	SMS to D:, instant update of SP2	2006-06-14	No
Server	CBCBES	Uninstalled SMS 2003 SP1 and SP2	2006-06-14	No
Server	CBCBES	COM + Reinstalled (Corrupted) --- IIS Services	2006-06-14	No
Server	CBCINTRANET	Completed Add, Update on local --> Transfer to CBC	2006-06-08	No

EMCBC RECORD OF REVISION

DOCUMENT

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

- Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.
- Placing the words GENERAL REVISION at the beginning of the text.

Rev. No.	Description of Changes	Revision on Pages	Date
1	Initial Procedure	All	01/29/07
2	Updated references	1	06/19/08
2	Added steps in section 8 and in form to determine if the change will impact Interconnect agreement or documents/procedures	5,8	06/19/08
2	Added Flowchart	7	06/19/08

CONTROLLED DOCUMENT CHANGE REQUEST

DATE: ____6/2/2008_____

INITIATOR: _____W.Best_____

INITIATOR PHONE NUMBER: __60530_____

DOCUMENT AFFECTED: Configuration Management of Computer Systems and Networks
_____

SECTION: __4.1_____ PARAGRAPH #:_____

CONTROLLED NUMBER : IP-240-02_____ PARAGRAPH #:_____

NEW CONTROLLED NUMBER: _IP-240-2, Rev 2_____

PROPOSED
REVISION: __Section 4.1, added new references to new SSP, added requirements to ensure that changes that affect interconnects or internal documents and procedures are identified. and to Comply with EMCBC Policies and Procedures new format.
_____
_____
_____

JUSTIFICATION: _Revising to align with cyber security requirements
_____
_____
_____
_____

Requested by:
__W.Best_____ DATE: ____6/2/2008_____

Approval:
_____ DATE: _____
Associate Director

Assigned to: _____ DUE DATE: _____

IP-250-01-F2, Rev.1

Document Review Record Sheet				
Document Title	Configuration Management of Computer Systems and Networks			
Control Number IP-240-02	Revision No. 2	Date Issued for Review 6/2/2008		
The subject document is being submitted for your review, approval or comments. Since this review is controlled, a response is required from all reviewers. Therefore, please return the review sheet with or without comments				
To: L. Chafin	Extension: 60461	By: 6/16/2008		
Additional Instructions:				
Reviewer	Approve	Approve w/Comments	Do Not Approve	Signature of Reviewer
B. Fain				
M. Roy				
W. Best				
L. Schlag				
H. Taylor				
R. Holland				
T. Brennan				
R. Everson				
T. J. Jackson				
J. Craig				
Comments may be attached to a separate sheet of paper				
APPROVE: Signifies the reviewer's acceptance of the document issued for review.				
APPROVE w/comments: Signifies the reviewer's overall acceptance of the document regarding concept, practice, implementation, provisions and assigned responsibilities. However, the reviewer has suggestions as to the organization of its contents or helpful additions and/or deletions. These comments are termed "non-mandatory comments" and do not require formal resolution between the reviewer and preparer.				
DO NOT APPROVE: Signifies that the reviewer has identified significant problems regarding concept, practice, implementation or responsibilities that render the document unacceptable and/or not in conformance with stated requirements. Such problem areas must be clearly identified by the reviewer. It is mandatory for the preparer to resolve these comments with the reviewer document the resolution and obtain the reviewers concurrence for the resolution. The reviewer's written concurrence with the resultant change in disposition shall be documented on this form.				
General Review Comments:				
When review is delegated, the designated reviewer shall review and indicate concurrence with the designee's review comments and recommend disposition:				
Designated Reviewer	Concur	Do Not Concur	Signature	Date

IP-250-01-F3, Rev.1